

MEMORANDUM FOR: Director of Central Intelligence

VIA: Deputy Director of Central Intelligence  
Deputy Director for Administration

FROM: [REDACTED]  
Director of Security

25X1

SUBJECT: Support to Foreign Intelligence Surveillance Court

1. Action Requested: None, for information.

25X1 2. Background: With your concurrence, we nominated [REDACTED] of the DCI Security Committee staff to be security officer for the U.S. Foreign Intelligence Surveillance Court. The Judges of that court so appointed him in May 1979 when the court began operations. Court security procedures require the security officer to conduct an annual security audit and report the result to the court.

25X1 3. Discussion: [REDACTED] audit report was sent by Presiding Judge Hart to his fellow court members and to Mr. Foley, the Director of the Administrative Office of the United States Courts. Mr. Foley in turn sent it to the Chief Judges of all United States Courts of Appeals and District Courts commending the soundness of the security advice and recommending it be heeded. A copy of Judge Hart's memorandum commending [REDACTED] work is attached.

I am pleased to have this opportunity to advise of this well merited recognition.

Should you wish to acknowledge Judge Hart's observation, I've attached a draft of a note for your consideration.

DOJ Review Completed

[REDACTED]

25X1

Attachments

cc: General Counsel w/atts

OS 0 2056

SUBJECT: Support to Foreign Intelligence  
Surveillance Court

Distribution:

Orig - Adse w/atts  
1 - DDCI w/atts  
1 - ER w/atts  
1 - OGC w/atts  
1 - DDA w/atts  
1 - D/SEC w/atts  
1 - OS Registry w/atts  
1 - DD/CA Subject  
① - DD/CA Chrono

DD/CA/ [redacted] (8 Aug 80)

25X1

The Honorable George L. Hart, Jr.  
United States District Court for  
the District of Columbia  
Washington, D.C. 20001

Dear Judge Hart:

I have seen your note recognizing  work25X1  
as your security advisor. I am glad my staff has been of  
help to the court. Please let me know if there is any  
additional assistance we can provide.

Yours sincerely,

STANSFIELD TURNER

The Honorable George L. Hart, Jr.  
United States District Court for  
the District of Columbia

Distribution:

Orig - Adse.  
1 - DCI  
1 - DDCI  
1 - ER  
1 - OGC  
2 - DDA  
2 - D/SEC  
1 - OS Registry  
1 - DD/CA Subject  
① - DD/CA Chrono

DD/CA/ [redacted] (11 Aug 80)

25X1

for the District of Columbia  
Washington, D. C. 20001

Chambers of  
George L. Hart, Jr.  
United States District Judge

August 5, 1980

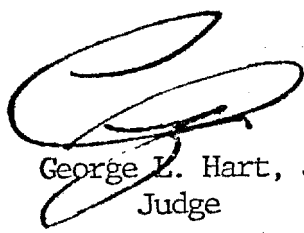
MEMORANDUM TO: Members of the U. S. Foreign Intelligence  
Surveillance Court

FROM: Judge Hart

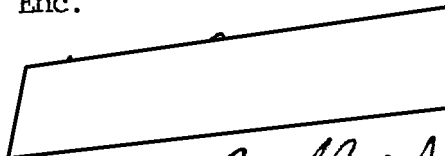
Under date of June 20, 1980, I forwarded to you a report of the annual security audit of our Court, as required by Public Law. This report was prepared by [redacted] our25X1 Court Security Officer. Attached to this report was a suggestion of "Security Lessons Learned".

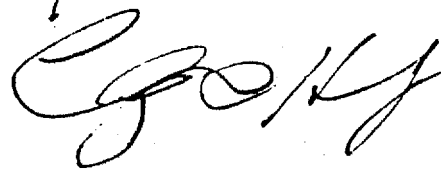
On the same date I forwarded a copy of "Security Lessons Learned" to Mr. Foley and suggested that it might be of use to the various federal Chief Judges throughout the country.

You will be interested to note the enclosed memorandum sent out by Mr. Foley, under date of July 28, 1980, to the federal Chief Judges. I consider same a feather in the cap of our Security Officer.

  
George L. Hart, Jr.  
Judge

Enc.



*I think you will  
find this of interest.*  


**WILLIAM E. FOLEY**  
DIRECTOR


**JOSEPH F. SPANIOL, JR.**  
DEPUTY DIRECTOR

**July 28, 1980**

**To the Chief Judges of the United States Courts  
of Appeals and United States District Courts:**

The enclosed report pertaining to security problems has recently been brought to our attention and I am sending it to you herewith for your information. The security suggestions contained in the report are sound. We recommend that the advice be heeded.

Sincerely yours,

  
**William E. Foley**  
Director

**Enclosure**

"Security Lessons Learned"

A recent criminal trial and conviction in a United States district court highlighted several potential security vulnerabilities with respect to safeguarding classified information. Some "security lessons learned" from this case include:

a. The covert placement in a government agency conference room of an electronic recording device shows the need to keep spaces where sensitive information is discussed secure when not in use, and to admit only persons with proper clearances and need-to-know for the subjects being discussed. Negative results from a technical survey for clandestine transmitters cannot provide assurance against either the pre-placement and later servicing, or the covert carrying into and out of a conference room of miniaturized recording devices.

b. The ease with which unauthorized persons entered private offices and removed and copied documents stored there shows the need to keep offices secured when not in use; to lock sensitive documents in a secure container; to keep official papers under direct observation when spaces are occupied; and to challenge unknown or unauthorized persons found in private offices.

c. The unauthorized use of official identification making equipment at a government agency, and the use of the resultant forged credentials to gain access to controlled areas, shows the need to require more than mere display of credentials before admitting a hitherto unknown person to a private office or providing him or her official papers.

One of the documents seized in this case was a detailed "how to" manual on entering government buildings and gaining access to private offices and official documents. Basing advice on the premise that a bold manner, cool nerves, and

reasonable preparation will get you into and out of wherever you want to go, the manual instructs agents to:

- a. Have a plausible story ready to justify your presence;
- b. locate a safe space (e.g., empty office) where you can wait until your target office is vacated;
- c. locate a reproduction machine and jimmy it "on" if locked;
- d. check the target office to see if it is vacant then use a credit card, piece of sheet metal, or length of flexible wire to "slip" the bolt on a locked door;
- e. look for keys to file cabinets or combinations to safes in such frequently used places as top middle drawers of nearby desks or file card boxes;
- f. locate the files of interest, leave the target office appearing as it was, go to the previously energized "xerox" machine and make your copies, then return the files, close the safes and re-lock the door; and
- g. walk out of the building with your copies, acting like a staff member who worked late and is taking material home to finish.

It worked for these agents. Much simpler versions of this sort of brazenness work for people who steal personal items or office equipment from buildings. The security lesson is lock it up, but don't leave the key or combination where others can find it; assure yourself that your spaces are adequately protected by good locks, working alarms and responsible guards; don't let unknown persons into your offices during working hours on the basis of vague explanations; and challenge people who don't seem to belong where they are.